Authenticated Encryption: Combining Authentication with Encryption to get IND-CCA

15-859I
Spring 2003

Motivation

- We have previously shown how to construct a symmetric encryption scheme, $SE$ which is secure against chosen-plaintext attacks, based on the assumption that one-way functions exist.
- We have introduced a provably stronger notion of security: indistinguishability under chosen ciphertext attack.
- Question: How can we construct a system which meets this notion?

Authenticated Encryption

- [BN00] Consider the problem of generically combining message authentication with encryption:
  - Develop two notions of authenticated encryption, INT-PTXT and INT-CTXT
  - Consider three ways to combine a MAC with an encryption scheme, and determine if the result satisfies INT-PTXT or INT-CTXT
  - Show that if $SE$ satisfies IND-CPA and INT-CTXT it also satisfies IND-CCA.

Punchline

- Let $(G,E,D)$ be a cryptosystem satisfying IND-CPA and let $(K,T,V)$ be a strongly unforgeable MAC. Then the cryptosystem $SE = (G',E',D')$ satisfies IND-CCA, where:
  - $G'(1^k) = K_e \leftarrow G(1^k); K_m \leftarrow K(1^k), (K_e,K_m)$
  - $E'(K_e,K_m,M) = \text{let } c = E(K_e,M), t = T(K_m,c), \text{return } (c,t)$
  - $D'(K_e,K_m,(c,t)) = \text{If } V(K_m,c,t) = 1 \text{ then } D(K_e,c), \text{ else } \bot$

Definitions: IND-CPA

Let $SE = (G,E,D)$ be a symmetric encryption scheme. Define $LR(b,x_0,x_1) = x_b$ if $|x_0| = |x_1|$, = otherwise.

$\text{Exp}_{A,SE}^{\text{cpa}}(k) = \text{Choose } K \leftarrow G(1^k)$
$\text{Return } A^{E_K(LR(b,\ldots))(1^k)}(1^k)$.

Define the advantage of $A$, $\text{Adv}_{A,SE}^{\text{cpa}}(k)$, by $\Pr[\text{Exp}_{A,SE}^{\text{cpa}}(k) = 1] - \Pr[\text{Exp}_{A,SE}^{\text{cpa}-0}(k) = 1]$
And $\text{Insec}_{SE}^{\text{cpa}}(k,t,q,l) = \max_{A^{E_K(LR(b,\ldots))(1^k)}}\{\text{Adv}_{A,SE}^{\text{cpa}}(k)\}$

Definitions: IND-CCA

Let $SE=(G,E,D)$
Define $\text{Exp}_{A,SE}^{\text{cca}}(k) =$ Choose $K \leftarrow G(1^k)$
Return $A^{E_K(LR(b,\ldots))(1^k)}(1^k)$.

A is not allowed to query $D_K$ on $C \leftarrow E_K(LR(b,\ldots))$.
Define the advantage of $A$, $\text{Adv}_{A,SE}^{\text{cca}}(k)$, by $\Pr[\text{Exp}_{A,SE}^{\text{cca}}(k) = 1] - \Pr[\text{Exp}_{A,SE}^{\text{cca}-0}(k) = 1]$
And $\text{Insec}_{SE}^{\text{cca}}(k,t,q,l) = \max_{A^{E_K(LR(b,\ldots))(1^k)}}\{\text{Adv}_{A,SE}^{\text{cca}}(k)\}$
Definitions: SUF-CMA

Let $MA = (K,T,V)$ be a MAC.
Define $Exp_{A,MA}^{suf-cma}(k) =$

$K \leftarrow K(1^k)$
If $A^{T_K,V_K}(1^k)$ queries $V_K(M,s)$ such that $V_K(M,s) = 1$ and $T_K(M)$ never returned $s$
then return 1, else return 0.
Define $Adv_{A,MA}^{suf-cma}(k) = Pr[Exp_{A,MA}^{suf-cma}(k) = 1]$,
$Insec_{MA}^{suf-cma}(k,t,q,l) = \max_A{Adv_{A,MA}^{suf-cma}(k)}$

SUF-CMA vs EUF-CMA

- Notice that this is a bit different from our previous definition of security for a MAC: before $A$ could only win if his message $M$ had not been queried previously. Now he wins if $s$ was never returned by $T(M)$.
- Any stateless, deterministic MAC satisfies SUF-CMA whenever it satisfies EUF-CMA.
- In particular, CBC-MAC extended to arbitrary message spaces satisfies SUF-CMA.

Integrity of Authenticated Encryption

- Authenticated encryption allows the decryption oracle to return the symbol ⊥ on an invalid ciphertext.
- Intuitively, a scheme has integrity of plaintexts if it is hard to make a valid ciphertext for a new plaintext, given access to an encryption oracle and a validity oracle $D_K^*$ that returns 1 if $D_K^*(C) = 1$.
- A scheme has integrity of ciphertexts if it is hard to make a new, valid ciphertext.

INT-PTXT

Define $Exp_{A,SE}^{int-plaintext}(k) =$

Choose $K \leftarrow G(1^k)$
if $A^{E_K,D_K^*}(1^k)$ queries $D_K^*(C)$ such that:
$D_K^*(C) = M \neq \perp$ and $E_K(M)$ was never queried
then return 1, else return 0.
Define $Adv_{A,SE}^{int-plaintext}(k) = Pr[Exp_{A,SE}^{int-plaintext}(k) = 1]$,
$Insec_{SE}^{int-plaintext}(k,t,q,l) = \max_A{Adv_{A,SE}^{int-plaintext}(k)}$

INT-CTXT

Define $Exp_{A,SE}^{int-ciphertext}(k) =$

Choose $K \leftarrow G(1^k)$
if $A^{E_K,D_K^*}(1^k)$ queries $D_K^*(C)$ such that:
$D_K^*(C) = M \neq \perp$ and $E_K$ never returned $C$
then return 1, else return 0.
Define $Adv_{A,SE}^{int-ciphertext}(k) = Pr[Exp_{A,SE}^{int-ciphertext}(k) = 1]$,
$Insec_{SE}^{int-ciphertext}(k,t,q,l) = \max_A{Adv_{A,SE}^{int-ciphertext}(k)}$

INT-CTXT ⇒ INT-PTXT

Theorem. If $SE=(G,E,D)$ is INT-CTXT secure it is also INT-PTXT secure:
$Insec_{SE}^{int-plaintext}(k,t,q,l) \leq Insec_{SE}^{int-ciphertext}(k,t,q,l)$
### Theorem: Let $SE=(G,E,D)$ and suppose $SE$ satisfies INT-CTXT and IND-CPA. Then it is secure against chosen-ciphertext attack:
\[
\text{Insec}_{SE}^{\text{ind-cca}}(k,t,q,l) \leq 2\text{Insec}_{SE}^{\text{int-ctxt}}(k,t,q,l) + \text{Insec}_{SE}^{\text{ind-cpa}}(k,t,q,l)
\]

**Proof:** (idea) Let $A$ be an IND-CCA adversary with high advantage. We will show how to construct an INT-CTXT adversary $A_c$ and an IND-CPA adversary $A_p$ such that at least one also has high advantage.

#### Adversaries $A_c$, $A_p$

- $A_c^{E_K,D_K^*}(1^k) = \begin{array}{ll}
    \text{Choose } b \leftarrow \{0,1\} \\
    \text{Run } A(1^k): \\
    \text{On query } E(M_0,M_1), \text{respond with } E_K(M_b) \\
    \text{On query } D(C): \text{if } D_K^*(C) = 1 \text{ then stop. else respond with } \bot
  \end{array}$

- $A_p^{E_K(LR(b,.,.))(1^k)} = \begin{array}{ll}
    \text{Run } A(1^k) \text{ to get } b': \\
    \text{On query } E(M_0,M_1), \text{respond with } E_K(LR(b,M_0,M_1)) \\
    \text{On query } D(C) \text{ respond with } \bot
  \end{array}$

#### Proof of IND-CCA Theorem

- For any event $X$, we use the notation:
  \[
  \Pr[X] = \Pr[X : b \leftarrow \{0,1\}, \text{Exp}_{A_{SE}^{\text{ind-cca}}}(k)]
  \]
  \[
  \Pr_i[X] = \Pr[X : \text{Exp}_{A_{SE}^{\text{int-ctxt}}}(k)]
  \]
  \[
  \Pr_r[X] = \Pr[X : b \leftarrow \{0,1\}, \text{Exp}_{A_{SE}^{\text{ind-cpa}}}(k)]
  \]
  \[
  \text{Call } b' \text{ the output of } A \text{ in } \text{Exp}_{A_{SE}^{\text{int-cca}}}(k).
  \]
  \[
  \text{Let } E \text{ be the event that } A \text{ submits a query } C \text{ such that } D_K(C) \neq \bot.
  \]
  Then \[
  \frac{1}{2} \text{Adv}_{A_{SE}^{\text{ind-cca}}}(k) + \frac{1}{2} = \Pr[b' = b] = \Pr[b' = b] + \Pr[b' = b] + \Pr[b' = b]
  \]
  \[
  \leq \Pr[E] + \Pr[b' = b] = \text{Adv}_{SE,A_{SE}^{\text{int-ctxt}}}(k) + \frac{1}{2}\text{Adv}_{SE,A_{SE}^{\text{ind-cpa}}}(k) + \frac{1}{2}
  \]

#### IND-CCA $\Rightarrow$ INT-PTXT

- Theorem: If there exists a scheme $SE = (G,E,D)$ which satisfies IND-CCA then there exists a scheme $SE'=(G',E',D')$ which satisfies IND-CCA but not INT-PTXT

- **Proof:** Define $G' = G$

  \[
  \text{E}'_K(M) = 0||E_K(M)
  \]
  \[
  \text{D}'_K(b||C) = \begin{cases} 
    1 & \text{if } (b = 0) \text{ then } \text{D}_K(C) \text{ else } 0 \\
    \text{Adversary } A(1^k) = \text{Query } D'_K(1||0). \\
    \text{Adv}_{A_{SE}^{\text{int-PTXT}}}(k) = 1.
  \end{cases}
  \]

  But given an oracle for $E'_K(LR(b,0,0))$ and one for $D'_K$, we can perfectly simulate same for $E'_K$, $D'_K$. Thus $SE'$ is IND-CCA secure iff SE is IND-CCA secure.

### How to combine a MAC and cipher

- There are several ways we could conceivably compose a MAC $(K,T,V)$ with a cryptoscheme $(G,E,D)$:
  - Encrypt-And-Mac: $E'(M) = E(M)||T(M)$
  - Mac-Then-Encrypt: $E'(M) = E(M)||T(M)$
  - Encrypt-Then-Mac: $E'(M) = E(M)||T(E(M))$

- Which is guaranteed to give us IND-CPA? IND-PTXT? IND-CTXT?

### Encrypt-and-MAC: IND-CPA?

- Theorem: For any secure, deterministic MAC, Encrypt-and-MAC is not IND-CPA secure.

- **Adversary:** Query $E_K(LR(b,0,0))$ to get $E_K(0)$, $T_K(0)$. Query $E_K(LR(b,0,1))$. If the tag is the same as the first, guess $b = 0$, else guess $b = 1$.

- (If the MAC is secure, then $T_K(0)=T_K(1)$ with only negligible probability)
Encrypt-and-MAC: INT-PTXT?

- Theorem: If MA is SUF-CMA then SE' = Encrypt-then-MAC is INT-PTXT secure: \( \text{Insec}_{\text{SE'}} \text{int-ptxt}(k,t,q,l) \leq \text{Insec}_{\text{MA}} \text{suf-cma}(k,t,q,l) \).
- Proof: Given a INT-PTXT adversary A for SE', we can simulate SE' given T,V oracles for MA by choosing a key for SE.
- Suppose A succeeds. Then A has produced a valid ciphertext \( C'=C,t \) for some message M that was never queried. Thus \( V(M,t)=1 \).
- Thus we succeed in forging MA whenever A succeeds in the INT-PTXT sense.

Encrypt-and-MAC: INT-CTXT?

- Theorem: If there exist SE which is IND-CPA secure and MA which is SUF-CMA, then there exists SE' such that SE' is IND-CPA secure but E&M(SE',MA) is not INT-CTXT secure.
- Proof: SE' = SE except \( E'(M) = 0||E(M) \), \( D'(b||C) = D(C) \). It is easy to see that SE' is still IND-CPA, but \( \text{Insec}_{E&M(SE,MA)} \text{int-ctxt}(k,O(1),1,1) = 1 \) since we can forge a new valid ciphertext by querying \( E(0) \) to get \( 0||C \) and returning \( 1||C \).

Mac-then-Encrypt: IND-CPA?

- Theorem: If SE is IND-CPA and MA is SUF-CMA then MtE(SE,MA) is IND-CPA:
- \( \text{Insec}_{\text{MtE}} \text{ind-cpa}(k,t,q,l+s) \leq \text{Insec}_{\text{SE}} \text{ind-cpa}(k,t,q,l) + \text{Insec}_{\text{MA}} \text{suf-cma}(k,t,q,l) \)
- Proof: Given a IND-CPA adversary A for MtE, we construct a IND-CPA adversary B for SE:
  - \( \text{B}^{\text{E}^{\text{E}}(\cdot)}(\cdot) : \text{Choose } K \leftarrow \text{MA.K}(1^k) \text{; Run A; respond to LR}(M_0, M_1) \text{ with LR}(M_0||T(M_0), M_1||T(M_1)) \text{; Return result of A.} \)
  - Clearly B has the same advantage as A.

MAC-then-Encrypt: INT-PTXT?

- Theorem: If MA is SUF-CMA secure then MtE(SE,MA) is INT-PTXT secure:
  - \( \text{Insec}_{\text{MtE}} \text{int-ptxt}(k,t,q,l) \leq \text{Insec}_{\text{SE}} \text{ind-cpa}(k,t,q,l+qs) \)
- Proof: Given a INT-PTXT adversary A, construct a SUF-CMA adversary B for MA:
  - \( \text{B}^{\text{E}^{\text{E}}(\cdot)}(\cdot) : \text{Choose } K \leftarrow \text{G}(1^k) \text{; Run A. On query } E(M), \text{ send } E_K(M||T(M)) \text{; On query } D^*(C), \text{ send } V(D_K(C)) \text{; Clearly if A succeeds in creating A valid ciphertext for an M which was never queried, B succeeds in finding a M,t pair where t was never output by T(M).} \)

Mac-then-Encrypt: INT-CTXT?

- Theorem: If there exist SE satisfying IND-CPA and MA satisfying SUF-CMA, then there exists SE' satisfying IND-CPA such that MtE(SE,MA) is not NM-CPA secure.
- Corollary: Since IND-CPA \( \land \text{INT-CTXT} \Rightarrow \text{NM-CCA} \Rightarrow \text{NM-CPA} \), we have that MtE is not INT-CTXT secure.
- Proof: SE' =
  - \( E'(M) = 0||E(M) \)
  - \( D'(b||C) = D(C) \)

Encrypt-then-MAC: IND-CPA?

- Theorem: If SE is IND-CPA secure then E&M(SE,MA) is IND-CPA secure:
  - \( \text{Insec}_{\text{E&M(SE,MA)}} \text{ind-cpa}(k,t,q,l) \leq \text{Insec}_{\text{SE}} \text{ind-cpa}(k,t,q,l) \)
- Proof: Given LR oracle for SE, we can perfectly simulate an LR oracle for E&M by choosing a key K, for MA:
  - \( \text{E&M.E(M)} = c \leftarrow E(M) \text{; return } c||T(c) \).
  - This simulation will succeed with the same success as an attack on SE.
Theorem: If MA is SUF-CMA secure then EtM(SE,MA) is INT-CTXT secure:
\[
\text{Insec}_{\text{EtM}}^{\text{int-ctxt}}(k,t,q,l) \leq \text{Insec}_{\text{MA}}^{\text{suf-cma}}(k,t,q,l+qs)
\]
where |SE.E(M)| = |M| + s

Proof: Given T,V oracles for MA, we perfectly simulate E,D* oracles for EtM by choosing a key K for SE and answering EtM.E(M) by letting c = SE.EK(M), t = T(c), and returning (c,t). Simulating D*(c,t) by V(SE.DK(c),t).

An INT-CTXT adversary A succeeds when it finds a C’ such that EtM.D*(C’) = 1 and C’ was not returned by EtM.E(). But in this case our simulation has also found a (c,t) pair such that V(c,t) = 1 and t was never returned by T(c). So we succeed in the SUF-CMA sense against MA.